


Finite Fields and Their Applications **6**, 119–129 (2000)

Article ID fta.1999.0268, available online at <http://www.idealibrary.com> on 

## Group Structure on Projective Spaces and Cyclic Codes over Finite Fields

Gilles Lachaud

*C.N.R.S. Institut de Mathématiques de Luminy, Case 930, F13288 Marseille Cedex 9, France*  
E-mail: [lachaud@iml.univ-mrs.fr](mailto:lachaud@iml.univ-mrs.fr)

Isabelle Lucien and Dany-Jack Mercier

*Equipe Applications de l'Algèbre et de l'Arithmétique de l'Université des Antilles et de la Guyane,  
Campus Fouillole, F97159 Pointe-à-Pître Cedex, France*  
E-mail: [isabelle.lucien@univ-ag.fr](mailto:isabelle.lucien@univ-ag.fr), [dany-jack.mercier@univ-ag.fr](mailto:dany-jack.mercier@univ-ag.fr)

and

Robert Rolland

*C.N.R.S. Institut de Mathématiques de Luminy, Case 930, F13288 Marseille Cedex 9, France*  
E-mail: [rolland@iml.univ-mrs.fr](mailto:rolland@iml.univ-mrs.fr)

*Communicated by Michael Tsfasman*

Received November 6, 1999; revised June 25, 1999

We study the geometrical properties of the subgroups of the multiplicative group of a finite extension of a finite field endowed with its vector space structure and we show that in some cases the associated projective space has a natural group structure. We construct some cyclic codes related to Reed–Muller codes by evaluating polynomials on these subgroups. The geometrical properties of these groups give a fairly simple description of these codes which are of the Reed–Muller kind. © 2000 Academic Press

*Key Words:* Error correcting codes, cyclic codes, Reed–Muller codes.

*AMS 1991 Mathematics Subject Classification:* 94B05.

### 1. INTRODUCTION—NOTATION

Let  $\mathbb{F}_q$  be the finite field with  $q$  elements. By an indexed subset of  $\mathbb{F}_q^n$  we mean a non-empty subset  $S$  of  $\mathbb{F}_q^n$  given with an enumeration  $S = \{s_1, \dots, s_t\}$ .

The subset  $S$  is indexed by  $\{1, \dots, l\}$ . We will denote by  $\mathbb{F}_q[x_1, \dots, x_n]$  the algebra of polynomials with  $n$  indeterminates and with coefficients in  $\mathbb{F}_q$ .

DEFINITION 1.1. Let  $F$  be a subspace of  $\mathbb{F}_q[x_1, \dots, x_n]$  and  $S = \{s_1, \dots, s_l\}$  an indexed subset of  $\mathbb{F}_q^n$ . The Reed–Muller code  $\text{RM}(F, S)$  is the image of the linear map

$$\begin{aligned} c: F &\rightarrow \mathbb{F}_q^l \\ f &\mapsto (f(s_1), \dots, f(s_l)). \end{aligned}$$

Note that the way in which the set  $S$  is indexed is important since our main interest is checking whether  $\text{RM}(F, S)$  is a cyclic code or not.

We denote by  $H_r$  the subspace of  $\mathbb{F}_q[x_1, \dots, x_n]$  of all homogeneous polynomials of degree  $r$  and the null polynomial ( $1 \leq r \leq n(q-1)$ ), and by

$$A_r = \bigoplus_{k=0}^r H_k$$

the subspace of all polynomials of degree at most  $r$ . With these definitions,  $\text{RM}(A_r, \mathbb{F}_q^n)$  represents the *generalized Reed–Muller code* of order  $r$  introduced by Kasami *et al.* and Delsarte *et al.* [3, 2], and  $\text{RM}(H_r, \mathbb{F}_q^n \setminus \{0\})$  is the *punctured homogeneous generalized Reed–Muller code* of order  $r$  defined by Moreno *et al.* [7].

Let  $\pi_n$  be the number of points of the projective space  $\mathbb{P}^n(\mathbb{F}_q)$  of dimension  $n$ . We have

$$\pi_n = \frac{q^{n+1} - 1}{q - 1} = 1 + q + q^2 + \dots + q^n.$$

Following Lachaud [5], a *projective generalized Reed–Muller code* is the image of the linear map

$$\begin{aligned} c: H_r &\rightarrow \mathbb{F}_q^{\pi_{n-1}} \\ f &\mapsto (f(s_1), \dots, f(s_{\pi_{n-1}})). \end{aligned}$$

where  $s_1, \dots, s_{\pi_{n-1}}$  are  $\pi_{n-1}$  fixed points of the punctured affine space  $\mathbb{F}_q^n \setminus \{0\}$ , each of them representing one and only one point in the projective space  $\mathbb{P}^{n-1}(\mathbb{F}_q)$ . Thus this code is nothing but the code  $\text{RM}(H_r, S)$  with  $S = \{s_1, \dots, s_{\pi_{n-1}}\}$ .

Moreover, our method leads to the following observation: If  $(q-1, n) = 1$ , then it is easy to see that the projective space  $\mathbb{P}^{n-1}(\mathbb{F}_q)$  has a natural group

structure. Assume now that  $(q - 1, n) > 1$ , then we calculate the largest (resp., the smallest) subgroup  $G \subset \mathbb{F}_q^*$  such that the restriction to  $G$  of the canonical map  $p : \mathbb{F}_q^n \setminus \{0\} \rightarrow \mathbb{P}^{n-1}$  is surjective (resp., injective). To this end we have to introduce the arithmetical function  $F(a, b)$  which is the greatest divisor of  $a$  which is relatively prime to  $b$ .

## 2. CYCLIC CODES

Let  $\alpha$  be a primitive element of the extension  $\mathbb{F}_{q^n}$  of degree  $n$  of  $\mathbb{F}_q$ . We know that  $(1, \alpha, \alpha^2, \dots, \alpha^{n-1})$  is a basis of the  $\mathbb{F}_q$ -vector space  $\mathbb{F}_{q^n}$ , and we use this basis to identify  $\mathbb{F}_{q^n}$  and  $\mathbb{F}_q^n$  as vector spaces. We denote by  $\mathbb{F}_q^*$  the multiplicative group  $\mathbb{F}_{q^n} \setminus \{0\}$ . Let  $\text{GL}(n, \mathbb{F}_q)$  be the linear group of order  $n$  over  $\mathbb{F}_q$ . A subspace  $F$  of  $\mathbb{F}_q[x_1, \dots, x_n]$  is called *invariant* if it is invariant under the action of the group  $\text{GL}(n, \mathbb{F}_q)$ , i.e.,  $f \circ T \in F$  if  $f \in F$  and  $T \in \text{GL}(n, \mathbb{F}_q)$ . The following simple lemma enables us to design many cyclic codes.

**LEMMA 2.1.** *Let  $F$  be an invariant subspace of  $\mathbb{F}_q[x_1, \dots, x_n]$  and let  $S = \{1, \theta, \dots, \theta^{l-1}\}$  be an indexed subgroup of the multiplicative group  $\mathbb{F}_q^*$ , of order  $l$  and generator  $\theta$ . Then the code  $\text{RM}(F, S)$  is cyclic.*

*Proof.* Let

$$c(f) = (f(1), f(\theta), \dots, f(\theta^{l-1}))$$

be a codeword of  $C = \text{RM}(F, S)$ . We must prove that

$$x = (f(\theta^{l-1}), f(1), f(\theta), \dots, f(\theta^{l-2}))$$

is also a codeword of  $C$ . The multiplication by  $\theta^{-1}$  defined an automorphism  $T$  of the  $\mathbb{F}_q$ -vector space  $\mathbb{F}_{q^n}$ , hence

$$\begin{aligned} x &= (f(\theta^{-1} \cdot 1), f(\theta^{-1} \cdot \theta), \dots, f(\theta^{l-1} \cdot \theta^{l-1})) \\ &= (f(T(1)), f(T(\theta)), \dots, f(T(\theta^{l-1}))) \end{aligned}$$

and  $x = c(f \circ T)$  belongs to  $C$  since  $f \circ T \in F$ . ■

Since  $A_r$  and  $H_r$  are invariant, we immediately get

**COROLLARY 2.1.** *Let  $\alpha$  be a primitive element of  $\mathbb{F}_{q^n}$  and  $S = \mathbb{F}_q^*$ . The codes  $\text{RM}(A_r, S)$  and  $\text{RM}(H_r, S)$  where  $S$  is indexed by*

$$S = \{1, \alpha, \dots, \alpha^{l-1}\}, \quad l = q^n - 1,$$

*are cyclic.*

These codes are respectively the punctured generalized Reed–Muller code and the punctured homogeneous generalized Reed–Muller code.

### 3. GEOMETRIC PROPERTIES OF SUBGROUPS OF $\mathbb{F}_q^*$

For each divisor  $k$  of  $q^n - 1$ , there is one and only one subgroup of  $\mathbb{F}_q^*$  of order  $k$ . From now on, we will denote by  $G_k$  this cyclic subgroup. The next result is standard.

**PROPOSITION 3.1.** *Let  $g_1$  and  $g_2$  be two divisors of  $q^n - 1$ . Then*

- $G_{g_1} \cap G_{g_2}$  is the subgroup of order  $\gcd(g_1, g_2)$ ,
- $G_{g_1} G_{g_2}$  is the subgroup of order  $\text{lcm}(g_1, g_2)$ .

In particular, the order of  $G_g \cap \mathbb{F}_q^*$  is  $w(g) = \gcd(g, q - 1)$ .

Let  $\theta$  be a generator of the cyclic subgroup  $G_g$  and  $l(g)$  be the smallest integer such that  $\theta^{l(g)}$  is in  $\mathbb{F}_q^*$ . Then the elements  $1, \theta, \dots, \theta^{l(g)-1}$  are on  $l(g)$  distinct lines  $D_0 = \mathbb{F}_q^*, D_1, \dots, D_{l(g)-1}$  and each  $D_i$  contains  $w(g)$  points of  $G_g$ ,

$$G_g \cap D_i = \{\theta^i, \theta^{l(g)+i}, \dots, \theta^{l(g)(w(g)-1)+i}\}.$$

hence

$$w(g) l(g) = g.$$

Note that  $\theta^{l(g)}$  is a generator of the group  $G_g \cap \mathbb{F}_q^*$ .

From now on, we call  $w(g)$  (resp.,  $l(g)$ ) the *width* (resp., *length*) of  $G_g$ .

**PROPOSITION 3.2.** *The width  $w(g)$  of  $G_g$  divides  $q - 1$ , and conversely, for each divisor  $s$  of  $q - 1$ , there is a subgroup  $G_g$  of width  $s$ .*

*The length  $l(g)$  of  $G_g$  divides  $\pi_{n-1}$ , and conversely, for each divisor  $r$  of  $\pi_{n-1}$ , there is a subgroup  $G_g$  of length  $r$ .*

*Proof.* From the definition, it is clear that  $w(g)$  divides  $q - 1$ . Now, we know that the order  $g$  of the subgroup  $G_g$  divides  $q^n - 1$ . Assume that  $g = (q^n - 1)/t$ . Then

$$w(g) = \gcd\left(\frac{q^n - 1}{t}, q - 1\right) = \frac{(q - 1)\gcd(\pi_{n-1}, t)}{t}$$

and

$$l(g) = \frac{g}{w(g)} = \frac{\pi_{n-1}}{\gcd(\pi_{n-1}, t)}.$$

Therefore,  $l(g)$  divides  $\pi_{n-1}$ . The subgroup  $G_s$  of  $\mathbb{F}_q^*$  has width  $s$ . The subgroup  $G_{r(q-1)}$  has length  $r$ . ■

For each divisor  $r$  of  $\pi_{n-1}$  and each divisor  $s$  of  $q-1$ , let us consider the sets

$$W(r) = \{w(g) \mid g \text{ divides } q^n - 1 \text{ and } l(g) = r\},$$

$$L(s) = \{l(g) \mid g \text{ divides } q^n - 1 \text{ and } w(g) = s\}.$$

By Proposition 3.2, these sets are not empty. Let us define

$$\omega(r) = \text{Min } W(r).$$

$$\lambda(s) = \text{Max } L(s).$$

The next result follows directly from the previous definitions:

PROPOSITION 3.3. *The sets  $W(r)$  and  $L(s)$  are also given by*

$$W(r) = \left\{ a \mid a \text{ divides } q-1 \text{ and } \gcd\left(\frac{q-1}{a}, r\right) = 1 \right\}$$

$$L(s) = \left\{ b \mid b \text{ divides } \pi_{n-1} \text{ and } \gcd\left(\frac{q-1}{s}, b\right) = 1 \right\}.$$

Let us denote by  $F(a, b)$  the greatest divisor of  $a$  which is relatively prime to  $b$ .

COROLLARY 3.1. *The bounds  $\omega(r)$  and  $\lambda(s)$  are given by*

$$\omega(r) = \frac{q-1}{F(q-1, r)},$$

$$\lambda(s) = F\left(\pi_{n-1}, \frac{q-1}{s}\right).$$

We now express some subgroups in analytic form using the norm.

Let  $N$  be the norm of the field extension  $\mathbb{F}_{q^n}$  over  $\mathbb{F}_q$ :

$$N(x) = x \cdot x^q \cdots x^{q^{n-1}} = x^{\pi_{n-1}}.$$

We know that  $N$  maps  $\mathbb{F}_q^*$  onto  $\mathbb{F}_q^*$  and that the kernel of  $N$  is the subgroup  $G_{\pi_{n-1}}$ .

PROPOSITION 3.4. *Let  $G_g$  be a subgroup of  $\mathbb{F}_q^*$ . If  $g = ab$  then*

$$G_g = \{x \in \mathbb{F}_q^* \mid x^a \in G_b\}.$$

*Proof.* The set on the right-hand side is the set of  $x \in \mathbb{F}_q^*$  such that  $x^{ab} = 1$ , and this set is the group of  $g$ th roots of unity  $G_g$ . ■

In particular, for  $g = \pi_{n-1}b$  we get

$$G_g = \{x \in \mathbb{F}_q^* \mid N(x)^b = 1\}.$$

#### 4. CONSTRUCTION OF CYCLIC CODES

Theorem 2.1 enables us to build many cyclic codes using subgroups of  $\mathbb{F}_{q^n}^*$  and the invariant polynomial subspaces  $A_r$  and  $H_r$ .

LEMMA 4.1. *We have the equality*

$$\gcd(\pi_{n-1}, q-1) = \gcd(n, q-1).$$

*Proof.* If  $d$  divides  $q-1$ , then  $q \equiv 1 \pmod{d}$  and

$$\pi_{n-1} = 1 + q + \cdots + q^{n-1} \equiv n \pmod{d},$$

hence  $d$  divides  $\pi_{n-1}$  if and only if  $d$  divides  $n$ . ■

As in Section 3, the width and the length of a subgroup  $G_g$  will be denoted by  $w(g)$  and  $l(g)$  respectively. From the previous lemma we get

PROPOSITION 4.1. *The width and the length of  $G_{\pi_{n-1}}$  are respectively*

$$w(\pi_{n-1}) = \gcd(q-1, n),$$

$$l(\pi_{n-1}) = \frac{\pi_{n-1}}{\gcd(q-1, n)}.$$

*Remarks.* In particular, if  $\gcd(q-1, n) = 1$  then  $w(\pi_{n-1}) = 1$  and  $l(\pi_{n-1}) = \pi_{n-1}$ .

Let us denote by  $p$  the canonical map from  $\mathbb{F}_q^*$  onto the projective space  $\mathbb{P}^{n-1}(\mathbb{F}_q)$ .

From the previous remark we deduce

**THEOREM 4.1.** *There is a subgroup  $G$  of  $\mathbb{F}_{q^n}^*$  such that the restriction of  $G$  of the map  $p$  is bijective if and only if  $\gcd(n, q - 1) = 1$ . In this case  $G = G_{\pi_{n-1}}$ .*

**COROLLARY 4.1.** *If  $\gcd(n, q - 1) = 1$  then there are cyclic generalized projective Reed–Muller codes of order  $r$ .*

*Proof.* It follows from Lemma 2.1 that if  $\gcd(n, q - 1) = 1$  then the subgroup  $G_{\pi_{n-1}}$  has one and only one point on each punctured vector line of  $\mathbb{F}_{q^n}^*$ . Therefore the code  $\text{RM}(H_r, G_{\pi_{n-1}})$  is a generalized projective Reed–Muller code. From Theorem 2.1 we conclude that this code is cyclic (with  $G_{\pi_{n-1}}$  indexed has explained in Section 2). ■

Hence in this case the projective space  $\mathbb{P}^{n-1}(\mathbb{F}_q)$  has a natural group structure.

If  $\gcd(n, q - 1) \neq 1$  then the subgroup  $G_{\pi_{n-1}} = \{x \mid N(x) = 1\}$  has width  $w(\pi_{n-1}) = \gcd(n, q - 1)$  (cf. Lemma 4.1) and the restriction to  $G_{\pi_{n-1}}$  of the map  $p$  is no longer bijective.

**THEOREM 4.2.** *Let  $H$  (resp.,  $H'$ ) be the largest (resp., smallest) subgroup of  $\mathbb{F}_q^*$  such that the restriction to this subgroup of the map  $p$  is injective (resp., surjective). Then*

$$H = G_{\lambda(1)}, \quad H' = G_{\pi_{n-1} \omega(\pi_{n-1})}$$

and

$$H \subset G_{\pi_{n-1}} \subset H'.$$

See Fig. 1.

*Proof.* The greatest  $g$  such that  $w(g) = 1$  satisfies  $l(g) = \lambda(1) = F(\pi_{n-1}, q - 1)$  by Corollary 3.1. Then  $g = \lambda(1)$ .

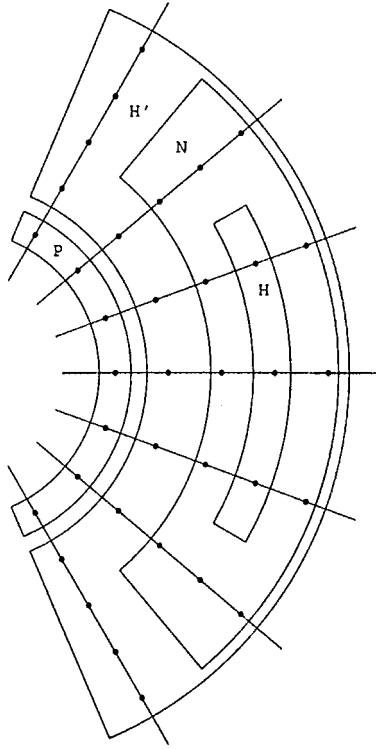
On the other hand, the smallest  $g'$  such that  $l(g') = \pi_{n-1}$  satisfies

$$w(g') = \omega(\pi_{n-1}) = (q - 1)/F(q - 1, \pi_{n-1}).$$

Then  $g' = \pi_{n-1} \omega(\pi_{n-1})$ . To get the inclusions, we just remark that  $\lambda(1)$  divides  $\pi_{n-1}$  and that  $\pi_{n-1}$  divides  $\pi_{n-1} \omega(\pi_{n-1})$ . ■

*Remark.* Let  $m = \gcd(n, q - 1)$ . If  $\pi_{n-1}$  is squarefree then  $H = G_{\pi_{n-1}/m}$ . If  $q - 1$  is squarefree then  $H' = G_{m\pi_{n-1}} = \{x \mid N(x)^m = 1\}$ .

If  $C$  is a  $[n, k, d]$ -code and  $\beta = (\beta_1, \dots, \beta_t) \in (\mathbb{F}_q^*)^t$ , let us define the  $[tn, k, td]$ -code  $\Phi(C, \beta)$  by the following construction. Starting with a codeword



**FIG. 1.** The lines are the open rays. We see the subgroups  $H, H', N = G_{\pi_{n-1}}$ .  $P$  represents the projective space.

$u = (u_1, \dots, u_n)$  of  $C$ , we build the codeword

$$\begin{aligned} v &= (v_1, \dots, v_m) \\ &= (\beta_1 u_1, \dots, \beta_1 u_n, \beta_2 u_1, \dots, \beta_2 u_n, \dots, \beta_t u_1, \dots, \beta_t u_n) \end{aligned}$$

of  $\Phi(C, \beta)$ .

**THEOREM 4.3.** *Let  $G_g$  be the indexed subgroup  $\{1, \theta, \dots, \theta^{g-1}\}$  of width  $w$  and length  $l$ . Let the subset  $S$  be the enumeration  $\{1, \theta, \dots, \theta^{l-1}\}$ . Then*

$$\text{RM}(H_r, G_g) = \Phi(\text{RM}(H_r, S), \beta),$$

where  $\beta = (1, \theta^l, \dots, \theta^{r(w-1)l})$ .



*Proof.* We construct a codeword  $v$  of  $\Phi(\text{RM}(H_r, S), \beta)$  starting from the codeword  $u = (P(1), P(\theta), \dots, P(\theta^{l-1}))$  of  $\text{RM}(H_r, S)$ . Then

$$v = (P(1), P(\theta), \dots, P(\theta^{l-1}), \dots, \theta^{r(w-1)l} P(1), \theta^{r(w-1)l} P(\theta), \dots, \theta^{r(w-1)l} P(\theta^{l-1})).$$

Since  $P$  is homogeneous of degree  $r$ ,

$$v = (P(1), P(\theta), \dots, P(\theta^{g-1})). \quad \blacksquare$$

Let us give some examples of this situation.

(a) The punctured homogeneous generalized Reed–Muller code  $\text{RM}(H_r, \mathbb{F}_{q^n}^*)$  of order  $r$  (cf. Section 1) can be constructed in this way, starting from the projective generalized Reed–Muller code  $\text{RM}(H_r, S_{\pi_{n-1}})$  (cf. Section 1) of order  $r$  where  $S_{\pi_{n-1}} = \{1, \theta, \dots, \theta^{\pi_{n-1}-1}\}$  and  $\theta$  is a generator of  $\mathbb{F}_{q^n}^*$ ,

$$\text{RM}(H_r, \mathbb{F}_{q^n}^*) = \Phi(\text{RM}(H_r, S_{\pi_{n-1}}), \beta),$$

where  $\beta = (1, \theta^{r\pi_{n-1}}, \dots, \theta^{r(q-2)\pi_{n-1}})$ .

(b) Let  $H'$  be the smallest subgroup of length  $\pi_{n-1}$  (cf. Theorem 4.2). The code  $\text{RM}(H_r, H')$  is obtained also from the projective generalized Reed–Muller code  $\text{RM}(H_r, S_{\pi_{n-1}})$  of order  $r$ ,

$$\text{RM}(H_r, H') = \Phi(\text{RM}(H_r, S_{\pi_{n-1}}), \beta),$$

where  $\beta = (1, \theta^{r\pi_{n-1}}, \dots, \theta^{r(\omega(\pi_{n-1})-1)\pi_{n-1}})$ .

In these two cases, we get a cyclic code from the projective generalized Reed–Muller code of order  $r$  which is not always cyclic. Hence the parameters of these two codes can be derived from the known parameters of the projective Reed–Muller code (cf. [5, 8]).

(c) Let  $G = G_{\pi_{n-1}} = \{x \mid N(x) = 1\}$  and  $m = \gcd(n, q-1)$ . The cyclic code  $\text{RM}(H_r, G)$  can also be built in this way, starting from the code  $\text{RM}(H_r, S)$  where  $S = \{1, \theta, \dots, \theta^{\pi_{n-1}/m-1}\}$  and  $\theta$  is a generator of  $G$ ,

$$\text{RM}(H_r, G) = \Phi(\text{RM}(H_r, S), \beta),$$

where  $\beta = (1, \theta^{r\pi_{n-1}}, \dots, \theta^{r(m-1)\pi_{n-1}})$ .

Note that the dimension and the minimal distance of the code  $\text{RM}(H_r, S)$  are not known. In particular, it would be useful to give a characterization of polynomials  $P$  such that  $P(x) = 0$  for every  $x \in S$ . (A similar problem is studied in [6].)

### 5. WEIGHTS OF CODE WORDS IN $\text{RM}(A_1, G_{\pi_{n-1}})$

The code  $\text{RM}(A_1, G_{\pi_{n-1}})$  is cyclic when it is defined with the enumeration of  $G_{\pi_{n-1}}$  given in Lemma 2.1. The set  $A_1$  is the space of polynomials of degree  $\leq 1$ , so each  $f \in A_1$  can be written as  $f = L + \mu$  where  $\mu \in \mathbb{F}_q$  and  $L \in H_1$  is a linear form on  $\mathbb{F}_q^n$ . Since  $\pi_{n-1} > q^{n-1}$  (i.e., the number of points of a hyperplane), the only element of  $A_1$  which is zero on  $G_{\pi_{n-1}}$  is the null polynomial. Hence the dimension of  $\text{RM}(A_1, G_{\pi_{n-1}})$  is  $n + 1$ .

If  $x, y \in \mathbb{F}_{q^n}$ , let

$$L_x(y) = \text{Tr}(xy),$$

where  $\text{Tr}: \mathbb{F}_{q^n} \rightarrow \mathbb{F}_q$  stands for the trace map from  $\mathbb{F}_{q^n}$  over  $\mathbb{F}_q$  defined by

$$\text{Tr}(x) = x + x^q + \cdots + x^{q^{n-1}}.$$

The trace map  $\text{Tr}$  is surjective. We also known that the bilinear map  $\text{Tr}(xy)$  is nondegenerate (cf. [1, A, V.47]), and this implies that the map

$$\begin{aligned} \mathbb{F}_{q^n} &\rightarrow H_1 \\ x &\mapsto L_x \end{aligned}$$

is an isomorphism of  $\mathbb{F}_q$ -vector spaces. So.

$$A_1 = \{L_x + \mu \mid x \in \mathbb{F}_{q^n} \text{ and } \mu \in \mathbb{F}_q\}.$$

Let  $f = L_x + \mu \in A_1$ , and  $Z(f) = \{y \in G_{\pi_{n-1}} \mid f(y) = 0\}$  represents the set of zeros of  $f$ . Then

$$\#Z(f) = \#\{y \in \mathbb{F}_{q^n} \mid N(y) = 1 \text{ and } \text{Tr}(xy) + \mu = 0\}$$

and we get

**THEOREM 5.1.** *If  $x \in \mathbb{F}_{q^n}$  and  $\mu \in \mathbb{F}_q$ , let*

$$M(x, \mu) = \#\{y \in \mathbb{F}_{q^n} \mid N(y) = 1 \text{ and } \text{Tr}(xy) + \mu = 0\}.$$

*If  $f = L_x + \mu \in A_1$ , the coweight of  $c(f) \in \text{RM}(A_1, S_1)$  is equal to  $M(x, \mu)$ , and the weight of  $c(f)$  is*

$$\text{weight}(c(f)) = \pi_{n-1} - M(x, \mu).$$

From Katz [4] we get:

**THEOREM 5.2.** *If  $x \in \mathbb{F}_{q^n}^*$  and  $\mu \in \mathbb{F}_q$ ,*

$$\left| M(x, \mu) - \frac{q^n - 1}{q(q-1)} \right| \leq nq^{n/2}.$$

Thus if  $f = L_x + \mu \in A_1$ , we deduce

$$\left| \text{weight}(c(f)) - \frac{q^n - 1}{q} \right| \leq nq^{n/2}$$

and then we get the following result:

**THEOREM 5.3.** *The parameters of  $C = \text{RM}(A_1, G_{\pi_{n-1}})$  are*

$$\text{length } C = \pi_{n-1}, \quad \dim C = n + 1, \quad \text{dist } C \geq q^{n-1} - \frac{1}{q} - nq^{n/2}.$$

## REFERENCES

1. N. Bourbaki, "Algèbre," *Éléments de Mathématiques*, Masson, Paris, 1981.
2. P. Delsarte, J. M. Goethals, and F. J. MacWilliams, On generalized Reed–Muller codes and their relatives, *Inform. and Control* **16**, No. 5 (1970), 403–442.
3. T. Kasami, S. Lin, W. W. Peterson, New generalizations of the Reed–Muller codes, *IEEE Trans. Inform. Theory* **IT-14**, No. 2 (1968) 189–205.
4. N. Katz, Estimates for Soto–Andrade sums, *J. Reine Angew. Math.* **438** (1993), 143–161.
5. G. Lachaud, The parameters of projective Reed–Muller codes, *Discrete Math.* **81** (1990), 217–221.
6. D.-J. Mercier and R. Rolland, Polynômes Homogènes qui s'annulent sur l'espace projectif  $\mathbb{P}^n(\mathbb{F}_q)$ , *J. Pure Appl. Algebra* **124** (1998) 227–240.
7. O. Moreno, Y. Duursma, J.-P. Cherdieu, A. Edouard, Cyclic subcodes of generalized Reed–Muller codes, *IEEE Trans. Inform. Theory* **44**, No. 1 (1998) 307–311.
8. A. B. Sørensen, Projective Reed–Muller codes, *IEEE Trans. Inform. Theory* **IT-37**, No. 6 (1991), 1567–1576.